AUTOMATIC RECOGNITION SYSTEM FOR USE IN A WIRELESS LOCAL AREA NETWORK (LAN)

This application claims priority of Taiwanese application no. 092121215, filed on July 31, 2003.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to a method and a system for automatically detecting a new joining portable device in a wireless local area network (LAN). It is able to confirm and update a user's operation status corresponding to the new joining portable device and provide suitable services according to the user's demand.

2. Description of the Prior Art

High-speed wireless LANs can provide the benefits of network connectivity without the restrictions of being tied to a location or tethered by wires. Wireless connections can extend or replace a wired infrastructure in situations where it is costly or prohibitive to lay cables. Temporary installations represent one example of when a wireless network might make sense or even be required. Some types of buildings or building codes may prohibit the use of wiring, making wireless networking an important alternative.

And of course the "no new wires" phenomenon involving wireless, along with phone line networking and even electrical power line networking, has become a major catalyst for home networking and the connected home experience.

The increasingly mobile user becomes a clear candidate for a wireless LAN. Portable access to wireless networks can be achieved using laptop computers and wireless Network Interface Cards (NICs). This enables the user to travel to various locations such as meeting rooms, hallways, lobbies, cafeterias, classrooms, etc. and still have access to their networked data. Without wireless access, the user would have to carry clumsy cabling and find a network tap to plug into.

Beyond the corporate campus, access to the Internet and even corporate sites could be made available through public wireless "hot spots" networks. Airports, restaurants, rail stations, and common areas throughout cities can be provisioned to provide this service. When the traveling worker reaches his or her destination, perhaps meeting a client at their corporate office, limited access could be provided to the user through the local wireless network. The network can recognize the user from another corporation and create a connection that is isolated from local corporate network but provides Internet access to the visiting user.

There are currently two prevalent wireless LAN solutions being deployed. These are the IEEE 802.11 standards, primarily 802.11b, which is referred to as Wi-Fi™, and the solution proposed by the HomeRF™ working group. These two solutions are not interoperable with each other or with other wireless LAN solutions. While HomeRF™ is designed exclusively for the home environment, Wi-Fi™ is designed for and is being deployed in homes, small and medium size businesses, large enterprises, and a growing number of public wireless networking hot spots. Several major laptop vendors are shipping or

are planning to ship laptops with internal Wi-Fi™ NICs.

Microsoft also partnered with 802.11 NIC vendors to improve the roaming experience by automating the process of configuring the NIC to associate with an available network.

The wireless NIC and its NDIS driver need to do very little beyond supporting a few new NDIS Object Identifiers (OIDs) used for the querying and setting of device and driver behavior. The NIC will scan for available networks and pass those to Windows XP. Windows XP has a Wireless Zero Configuration service that then takes care of configuring the NIC with an available network. In the case where there are two networks covering the same area. The user can configure a preferred network order and the machine will try each network in order until it finds an active one. It is even possible to limit association to only the configured, preferred networks.

If no 802.11 networks are found nearby, Windows XP will configure the NIC to use ad hoc networking mode. It is possible for the user to configure the wireless NIC to either disable or be forced into ad hoc mode. These zero configuration enhancements are integrated with the security enhancements such that if authentication fails, another network will be located to attempt association with.

Zero configuration is a client-based user identification method. Zero configuration allows wireless devices to work in different modes without the need for configuration changes after the initial configuration. The zero configuration initiative automatically provides the IP address, the network prefix, the gateway router location, the DNS server address, the address of a Remote

Authentication Dial In User Service (RADIUS) or Internet Authentication Service (IAS) server, and all other necessary settings for the wireless device. It also provides security features for the client.

Wireless LANs are built using two basic topologies. These topologies are variously termed; including managed and unmanaged, hosted and peer-to-peer, and infrastructure and ad-hoc.

An infrastructure topology is one that extends an existing wired LAN to wireless devices by providing a base station (called an access point). The access point bridges the wireless and wired LAN and acts as a central controller for the wireless LAN. The access point coordinates transmission and reception from multiple wireless devices within a specific range; the range and number of devices depend on the wireless standard being used and vendor's product. In infrastructure mode there may be multiple access points to cover a large area or only a single access point for a small area such as a single home or small building.

An ad-hoc topology is one in which a LAN is created solely by the wireless devices themselves, with no central controller or access point. Each device communicates directly with other devices in the network rather than through a central controller. This is useful in places where small groups of computers might congregate and not need access to another network. For example, a home without a wired network, or a conference room where teams meet regularly to exchange ideas, are examples of where ad-hoc wireless networks might be useful.

For example, when combined with today's new generation of smart peer-to-peer software and solutions, these ad hoc wireless networks can enable traveling users to collaborate, play multiplayer games, transfer files or otherwise communicate with one another using their PCs or smart devices wirelessly.

The laptop or smart device, which is characterized as a "station" in wireless LAN parlance, first has to identify the available access points and networks. This is done through monitoring for "beacon" frames from access points announcing themselves, or actively probing for a particular network by using probe frames.

The station chooses a network from those available and goes through an authentication process with the access point. Once the access point and station have verified each other, the association process is started. Association allows the access point and station to exchange information and capabilities. The access point can use this information and share it with other access points in the network to disseminate knowledge of the station's current location on the network. Only after association is complete can the station transmit or receive frames on the network.

In infrastructure mode, all network traffic from wireless stations on the network goes through an access point to reach the destination on either the wired or wireless LAN. Access to the network is managed using a carrier sense and collision avoidance protocol. The stations will listen for data transmissions for a specified period of time before attempting to transmit - this is the carrier sense portion of the protocol. The station must wait a specific period of time after the network becomes clear before

transmitting. This delay, plus the receiving station transmitting an acknowledgement indicating a successful reception form the collision avoidance portion of the protocol. Note that in infrastructure mode, either the sender or receiver is always the access point.

Because some stations may not be able to hear each other, yet both still be in range of the access point, special considerations are made to avoid collisions. This includes a kind of reservation exchange that can take place before a packet is transmitted using a request to send and clear to send frame exchange, and a network allocation vector maintained at each station on the network. Even if a station cannot hear the transmission from the other station, it will hear the clear to send transmission from the access point and can avoid transmitting during that interval.

The process of roaming from one access point to another is not completely defined by the standard. But, the beaconing and probing used to locate access points and a re-association process that allows the station to associate with a different access point, in combination with other vendor specific protocols between access points provides for a smooth transition.

Synchronization between stations on the network is handled by the periodic beacon frames sent by the access point. These frames contain the access point's clock value at the time of transmission so can be used to check for drift at the receiving station. Synchronization is required for various reasons having to do with the wireless protocols and modulation schemes.

Having explained the basic operation for infrastructure mode, ad-hoc mode can be explained by simply saying there is no access point. Only wireless devices are present in this network. Many of the responsibilities previously handled by the access point, such as beaconing and synchronization, are handled by a station. Some enhancements are not available to the ad-hoc network, such as relaying frames between two stations that cannot hear each other.

Besides Windows XP, several computer products have been also developed according to Zero configuration such as the servers, e220ET, e220ST, e220XP and e230SX, having three characteristics, zero install, zero configuration and zero operation. The servers respectively satisfy with the user's demands for small-sized network, middle-sized network, large-sized network and large-sized network with requesting mass storage. For the clients, who need a server to establish their own network but have no ability to maintain, they merely need one CD to easily complete auto installation of operation system (OS), monitor software and network management software by themselves. After inputting Internet Protocol (IP) address through control panel of the server, the clients can begin to use the server. Furthermore, by setting on the control panel, the clients may also easily configure their LAN environment to obtain www service, proxy service, Domain Name System (DNS) service, mail service, File Transfer Protocol (FTP) service, and Network Files System (NFS) service et al.

The present invention referred to the art as disclosed in US 6,327,535 providing a system for locating exterior computer device. The system processes location confirmation and data transmission for certain specific joining portable device by a host and plurality

of "Beacon" through wireless LAN.

In accordance with conventional design as mentioned above, the clients must input their own IP address before operating a server and thereby access a LAN. Basically, such design applies to charging mechanism of a wireless network service provider when it provides users wireless network services or security mechanism used in a server for preventing hacker. The users may select one of the sets of available service set identifier (SSID) when entering a wireless network environment. For the encryption of the wireless network, the users should further set Wired Equivalent Privacy (WEP) key. The WEP algorithm is used to protect wireless communication from eavesdropping. The other function of WEP is to prevent unauthorized access to a wireless network.

SUMMARY OF THE INVENTION

Actually, it is unnecessary to emphasize the certification procedure when establishing a home wireless LAN. Repeated certification procedure will obsess home users. Therefore, the object of the present invention is to provide a solution for omitting unnecessary input operation for certification, thereby simplify the home wireless LAN. In ideal condition, user's portable device may be readily detected through access point (AP) by a server in the home wireless LAN when the user actuates it. Then, the server can automatically complete all necessary settings of accessing the wireless LAN for the portable device and provide it with all available services in the wireless LAN.

In the wireless LAN, the server may utilize several wireless

transmission channels, such as IEEE 802.11 standards or Infrared Data Association (IrDA), to confirm and update the status of user's portable device as well as provide suitable information services corresponding to the user's demand, when receiving new joining device information from an access point.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig.1 is a configuration diagram according to the present invention.

Fig.2 is a derivational configuration diagram according to the present invention.

Fig.3 - Fig.5 are flow chart diagrams according to the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

Please refer to Fig.1 that shows a server 7 connecting with an access point (AP) module. The AP module comprises two access points, AP1 and AP2. An existing portable device U1 employs an existing wireless LAN and the server 7 to process data exchange through the access point AP1. In the existing wireless LAN, when a new joining portable device U2 is actuated, a wireless NIC connecting therewith will send a built-in service set identifier (SSID) of the portable device U2 to the access point (AP1 or AP2). Then, the access point sends the built-in SSID to the server 7 for recognition. The server 7 will temporarily cut off a connection between the server and the portable device U1 in the existing wireless LAN and select one set from a plurality of IP address retained in the server 7 for establishing a new connection with the portable device U2 when receiving the built-in SSID. For example, suppose system name of

initial SSID used by the server 7 is "MyHome", the server 7 will retain a plurality of SSID whose system name is MyHome for new adding. When the server 7 confirms that system name of the built-in SSID is not MyHome, all connections in the existing wireless LAN will be temporarily cut off by the server for example the server 7 temporarily cut off the connection with the portable device U1; meanwhile selecting one set of IP address retained in the server 7 whose SSID system name is MyHome for establishing a new connection with the portable device U2.

After establishing a new connection with the portable device U2, the server 7 use the initial SSID to re-connect with the portable device U1 and transmit all necessary information in the existing wireless LAN to the portable device U2. Once the portable device U2 receive the information, it will temporarily terminate an original setting of IP address therein and use the information from the server 7 whose SSID system name is MyHome to substitute the original setting of IP address. The information from the server 7 whose SSID system name is MyHome includes a set of IP address, Wired Equivalent Privacy (WEP) key and subsystem identification. Therefore, the portable device U2 can automatically join the existing wireless LAN without inputting authentication.

Fig.2 illustrates a derivational configuration diagram in accordance with the present invention. It is able to employ infrastructure topology to extend an existing wired LAN to wireless devices by the server 7 and the access point AP2. The access point AP2 bridges the wireless and wired LAN and acts as a central controller for the wireless LAN. The access point AP2 can coordinate transmission and reception from multiple wireless devices within

a specific range. The range and number of devices depend on the wireless standard being used and vendor's product. For example, it is able to connect with a desktop computer 11 or a printer 12 through the server 7, or connect with a TV through a Set top box 13. In infrastructure topology mode there may be multiple access points to cover a large area or only a single access point for a small area such as a single home or small building. Besides, it is also able to use ad-hoc topology. The ad-hoc topology is one in which a LAN is created solely by the wireless devices themselves, with no central controller or access point. Each device communicates directly with other devices in the network rather than through a central controller. This is useful in places where small groups of computers might congregate and not need access to another network.

Fig.3 - Fig.5 are flow chart diagrams in accordance with the present invention. The flow path includes the following steps:

Firstly, please refer to Fig.3.

(1) a server retain a plurality of initial SSID having specific system name for new adding (step S2);

(2) when a new joining portable device is actuated in an existing wireless LAN, a wireless NIC coupling therewith send out a built-in SSID of the new joining portable device (step S3);

(3) receiving the built-in SSID by an access point (step S4);

(4) transmitting the built-in SSID from the access point to the server (step S5);

Next as shown in Fig.4:

(5) recognizing the built-in SSID by the server (step S7);

(6) the server temporarily cut off a connection between the server and an existing portable device in the existing wireless LAN when the built-in SSID does not conform with initial SSID of the

server (step S8)

(7) the server use an IP address retained therein to establish a new connection with the new joining portable device through the access point (step S9);

(8) the new joining portable device temporarily terminate built-in IP address thereof when receiving the IP address from the server (step S10);

Next as shown in Fig.5:

(9) the new joining portable device replace the built-in IP address thereof with the IP address from the server (step S12);

(10) the new joining portable device connect with the server through the access point in the existing wireless LAN (step S13);

(11) re-connecting the existing portable device and the server in the existing wireless LAN (step S14).